

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US05/007535

International filing date: 08 March 2005 (08.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/551,320
Filing date: 08 March 2004 (08.03.2004)

Date of receipt at the International Bureau: 07 March 2005 (07.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

1303068

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

March 31, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: 60/551,320

FILING DATE: *March 08, 2004*

RELATED PCT APPLICATION NUMBER: *PCT/US05/07535*



Certified by

Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

Please type a plus sign (+) inside this box



Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

INVENTOR(S)

| | | |
|--|------------------------|---|
| Given Name (first and middle [if any]) | Family Name or Surname | Residence (City and either State or Foreign Country) |
| John J. | Giobbi | 689 NW Stonepine Drive, Bend, OR 97701 |

☐ Additional inventors are being named on the * separately numbered sheet attached hereto.

TITLE OF THE INVENTION (280 characters max)

Linked Account System Using Personal Digital Key (PD~~K~~LAS)

Direct all correspondence to:

CORRESPONDENCE ADDRESS

☐ Customer Number

OR

Type Customer Number here

| | | | | | |
|---|-----------------------|-----------|--------------|-----|--------------|
| <input checked="" type="checkbox"/> Firm or Individual Name | Michael J. Blankstein | | | | |
| Address | 2014 Harrison Street | | | | |
| Address | * | | | | |
| City | Evanston | State | Illinois | ZIP | 60201 |
| Country | USA | Telephone | 847/332-1304 | Fax | 847/332-1306 |

ENCLOSED APPLICATION PARTS (CHECK ALL THAT APPLY)

| | | | |
|---|---|---|---|
| <input checked="" type="checkbox"/> Specification Number of Pages | 5 | <input type="checkbox"/> CD(s), Number | |
| <input checked="" type="checkbox"/> Drawing(s) Number of Sheets | 2 | <input checked="" type="checkbox"/> Other (specify) | Appendix - Specification (32 pages) and Drawings (13 pages) |
| <input type="checkbox"/> Application Data Sheet. See 37 CFR 1.76. | | | |

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISION APPLICATION FOR PATENT (check one)

| | | |
|---|---------------------------|-------|
| <input checked="" type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27. | FILING FEE AMOUNT (\$) | |
| <input checked="" type="checkbox"/> A check or money order is enclosed to cover the filing fees. | | |
| <input type="checkbox"/> The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: | | |
| <input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached. | (*) | 80.00 |

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

Date March 8, 2004

SIGNATURE

Michael Blankstein

REGISTRATION NO.
(Attorney/Agent)

37097

TYPED or PRINTED NAME

Michael J. Blankstein

Docket Number

MD-7

TELEPHONE

847/332-1304

EXPRESS MAIL MAILING LABEL

NUMBER: EF284099775US

Date: March 8, 2004

I hereby certify that this paper or fee is being deposited with the United States Postal Service "EXPRESS MAIL POST OFFICE TO ADDRESSEE" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to Mail Stop Provisional Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature

Michael Blankstein

Typed Name

Michael J. Blankstein

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you

PATENT

PROVISIONAL APPLICATION FOR PATENT

for

**LINKED ACCOUNT SYSTEM USING PERSONAL DIGITAL KEY
(PDK-LAS)**

by

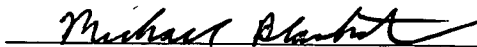
John J. Giobbi

EXPRESS MAIL MAILING LABEL

NUMBER EF284099775US

DATE OF DEPOSIT March 8, 2004

I hereby certify that this paper or fee is being deposited with the United States Postal Service "EXPRESS MAIL POST OFFICE TO ADDRESSEE" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to: Mail Stop Provisional Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.



Signature

Background:

With the advent of the Internet, and the online shopping, banking, etc. the Internet has enabled, the incidence of credit card, bank account information, and similar data being stolen has risen dramatically. The cost to providers of transactions performed with these stolen items is enormous and results in higher transaction fees and product pricing to consumers (as it is the *providers* who are typically responsible for charges applied to stolen account information).

Additionally, the inconvenience and tangential problems victims (consumers) suffer as a result of such crimes are often traumatic, but are minimally troublesome. The insufficient technologies and procedures currently utilized to secure account-based transaction processing do little to prevent these crimes. The problem is most notable in the case of the largest growing segment for such transactions, the on-line environment. The PDK-LAS technology is intended to directly address these security issues.

Note: See **Terminology** section at end of document for descriptions of important terms.

Summary:

The underlying concept of the PDK-LAS is that of linking a PDK-Key to a credit/debit card account, bank account, membership account, or any similar type of account for the purpose of providing user authentication to transactions involving the accounts, whether the transactions occur on-line or in-store.

A user of a PDK-LAS protected account is given a physical PDK-Key which must be present (in the vicinity) anytime a transaction involving the account is to occur. A PDK-Key may be similar to car fobs many people have on their key rings, and is intended to be carried in the same manner. Once in possession of a PDK-Key, a user registers the key with the manufacturer, and then assigns its use (typically over the Internet) to any provider account offering the PDK-LAS protection. The provider of an account to which the user has linked their PDK-Key will record (in their database) a record indicating the assignment between the account number and the associated PDK-Key.

When a transaction involving a PDK-LAS protected account takes place, in addition to transmitting the account number to a provider (as is currently done for nearly any account-based transaction), the PDK-Key wirelessly communicates with an RDC at a location of the user, and provides PDK-Key information that is also transmitted. Once the provider has received both the account number and the PDK-Key information, for authentication purposes, it verifies (via a search of its database) the transaction is indeed being performed by the individual the records indicate is associated with the account (the individual holding the physical key). An example of the effectiveness of this process is illustrated in the case of an account number stolen online (by eavesdropping on Internet transmissions, etc.). The account number will be un-usable to the perpetrators of the crime at any site employing the PDK-LAS technology because the perpetrators will not also possess the associated PDK-Key.

The passive, wireless design of the PDK technology means no interaction from users is required (other than to carry the keys in their pockets), and no appreciable delays to the transaction process are added. In effect, the PDK technology offers users and providers an efficient, passive, wireless technology capable of significantly enhancing the security of any account-based transaction process.

Providers, stores, and on-line sites utilizing the PDK-LAS technology benefit by preventing or greatly minimizing the number of transactions applied to illegally obtained account data. And as the technology becomes accepted and widely deployed, the added difficulty in benefiting from stolen account information will likely lessen the desire for such "robberies" to occur in the first place, minimizing the number of victimized users.

Detailed Description:

New PDK-Keys are sold independently or delivered with PDK hardware (PDK Hard Drive, RDC adapter, POS RDC) or linked accounts (credit/debit card account, bank accounts, membership accounts, or similar). Further information concerning such PDK hardware may be obtained from U.S. Patent Application Serial No. 10/715,035 filed November 17, 2003 and entitled "Digital Content Security System," which is attached hereto as an Appendix and incorporated herein by reference in its entirety. Once in possession of a PDK-Key, a user registers the key with the key manufacturer. No usage data (credit or bank account numbers, hard drive IDs, etc.) is maintained in the manufacturer's database - only user verification information. Such information likely includes: Customer account number (indicating the customer's record within the manufacturer's database), customer name, address and phone, key number, and status of key (in-use, stolen, lost, etc.). This information is used primarily for verification purposes during lost-key replacement procedures.

Once registered, a PDK-Key can be linked to PDK-protected objects and utilized as needed. See the next section for details of the procedures involved.

A PDK-Key used in the PDK-LAS technology is similar in every way to PDK-Keys defined in the aforementioned Serial No. 10/715,035. Secure RF communications between a PDK-Key and any RDC occurs in the same manner as defined in Serial No. 10/715,035. The data fields stored in PDK-Keys likely include:

- *User Label* - User text label [un-protected field]
- *Acct #* - User's manufacturer account number [protected field]
- *Key #* - Unique key ID (may be an encryption key, etc.) [protected field]

The PDK-Key communicates with one of three basic implementations of a PDK-RDC (other options may exist):

- *POS RDC* - Standard credit card swipe type-device with an integrated RDC
- *RDC Adapter* - Add-on PC board RDC (interfacing via USB, Firewire, PC Card, expansion slot, etc.)
- *PDK-Hard Drive* - Standard hard drive with an integrated RDC

POS RDC devices are primarily intended for in-store use (checkout lane, purchase counter, hand-held card swipes, etc.), while RDC Adapters or PDK-Hard Drives are primarily intended for PC-based use. Other options may exist in the future, but it is intended that any RDC device is capable of performing the procedures described herein.

Physical cards (credit/debit card account, bank accounts, membership accounts, or similar) intended for use with the PDK-LAS technology may be identical in every way to currently standard cards. No specific changes are required to such cards in order to ready them for use with the PDK-LAS technology. From a consumer standpoint, this feature (along with the ability for a PDK-Key to be purchased and assigned to an object at any point) enables easy acceptance of the technology.

Additionally, the PDK-LAS technology offers great flexibility in how PDK-Keys are distributed, assigned, and used. For example, providers may optionally allow dynamic key assignment (assigning of keys at a later date, assigning of multiple keys to the same account, etc.), and users may elect to use one PDK-Key for all their PDK-based security needs (one PDK-Key can be assigned to multiple accounts, PDK-Hard Drives, and other PDK-based products).

Standard Usage:

The sections below detail example transactions / procedures (first-time setup, purchases, on-line account access, etc.) pertaining to the use of the PDK-LAS technology. Minor variations to the procedures may exist in actual implementations; however the spirit and intent of the procedures remain relevant. {See diagrams #11 & #12}

User wishes to assign a key to a new PDK-Linked Account:

1. User logs on to provider's site (over Internet via user's personal computer) and inputs whatever validation provider typically requires (sufficient data must be requested by provider during this critical transaction to fully authenticate user)
2. RDC reads user's PDK-Key data and transmits data to provider
3. Provider confirms user's request to link PDK-Key to account
4. Once confirmed, PDK-Key data is permanently stored in provider's database as master PDK-Key (and can only be changed by directly contacting provider personnel)
5. **Note:** *Alternately, for this "setup" procedure, to facilitate users without an RDC-equipped PC and Internet access, users may phone providers directly and verbally relay all required information, including master PDK-Key data (printed on a card included with PDK-Key at purchase). For users with Internet access but no RDC, this information may be hand-entered on provider's website.*

User wishes to assign additional keys to a PDK-Linked Account:

1. User logs on to provider site and inputs whatever validation provider typically requires, *and* user must ensure assigned master PDK-Key is within vicinity of RDC
2. RDC reads master and additional PDK-Key data and transmits data to provider
3. Provider confirms user's request to link additional PDK-Key to account number (or change or remove keys, etc.)
4. Once confirmed, updated PDK-Key data is stored in provider's database along with master PDK-Key data
5. **Note:** *Alternately, for this "setup" procedure, to facilitate users without an RDC-equipped PC and Internet access, users may phone providers directly and verbally relay all required information, including both master and additional PDK-Key data (printed on cards included with PDK-Keys at purchase). For users with Internet access but no RDC, this information may be hand-entered on provider's website.*

User wishes to utilize a PDK-Linked Account to purchase a product at a store:

1. User must ensure an assigned PDK-Key is within vicinity of POS RDC at checkout counter
2. RDC reads user's PDK-Key and transmits data, along with user's account number (acquired using currently accepted procedures), to provider for verification (if more than one PDK-Key is read at counter: either data from all PDK-Keys can be transmitted to provider, or User Labels can be displayed on POS RDC to enable user or clerk to select appropriate PDK-Key)
3. Provider looks up account record in its database using transmitted account number, and compares transmitted PDK-Key data to information stored in record
4. If match is confirmed, sales transaction is completed normally (if not confirmed, transaction cannot be completed)

Standard Usage (continued):

User wishes to utilize a PDK-Linked Account to purchase a product on-line (or to access account's info on-line):

1. User must ensure an assigned PDK-Key is within vicinity of RDC
2. RDC reads user's PDK-Key and transmits data, along with user's account number (acquired using currently accepted procedures), to provider for verification (if more than one PDK-Key is read at RDC: either data from all PDK-Keys can be transmitted to provider, or User Labels can be displayed on computer screen to enable user to select appropriate PDK-Key)
3. Provider looks up account record in its database using transmitted account number, and compares transmitted PDK-Key data to information stored in record
4. If match is confirmed, transaction / session is completed normally (if not confirmed, transaction / session cannot be completed)

User loses a key:

- After initial master PDK-Key setup, users are encouraged to immediately assign an additional PDK-Key (which likely serves as day-to-day key) and store master PDK-Key in a safe location; if day-to-day key is lost, master can be used to assign new day-to-day key
- As a last resort, for users having lost all PDK-Keys, key manufacturer (either directly or via reseller of protected product) can be contacted and, after authentication is performed, instructed to ship replacement PDK-Key

Terminology:

- *PDK-Linked Account* - a bank, credit card, membership, or similar account linked to a PDK-Key
- *PDK-Hard Drive* - a physical or "electronic" hard drive containing an integrated RDC
- *PDK-protected product / object* - Hard drive or account protected via PDK technology
- *PDK-Key or Key* - a PDK-compliant wireless key providing access to PDK-protected objects
- *Assigned key* - PDK-Key assigned to one or more protected objects
- *RDC* - Reader/Decoder Circuit installed in a user's computer (or built into computer hard drive, etc.) or point-of-sale (POS) credit-card swipe unit which communicates with PDK-Keys and decodes PDK data
- *POS RDC* - Reader/Decoder Circuit integrated in a standard point-of-sale (POS) credit-card swipe unit
- *Manufacturer* - a manufacturer of PDK-Keys
- *Provider* - an entity issuing a PDK-Linked Account, PDK-Hard Drives, etc.
- *Customer or User* - an individual possessing / utilizing a PDK-Key
- *Master* - a PDK-Key initially assigned to a PDK-protected object, and which is required to be present for configuration transactions
- *Additional* - PDK-Keys assigned to a PDK-protected object in addition to master

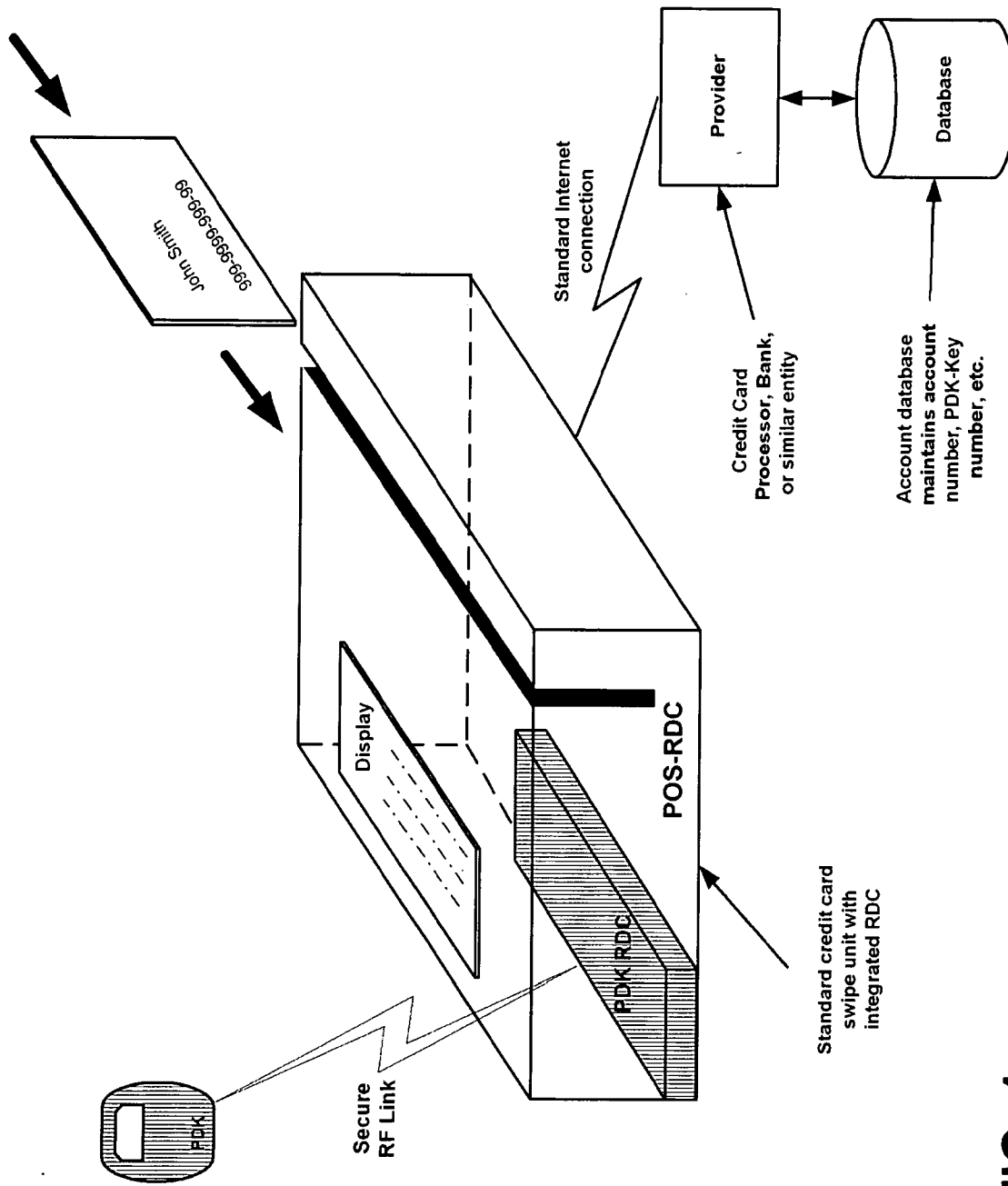


FIG. 1

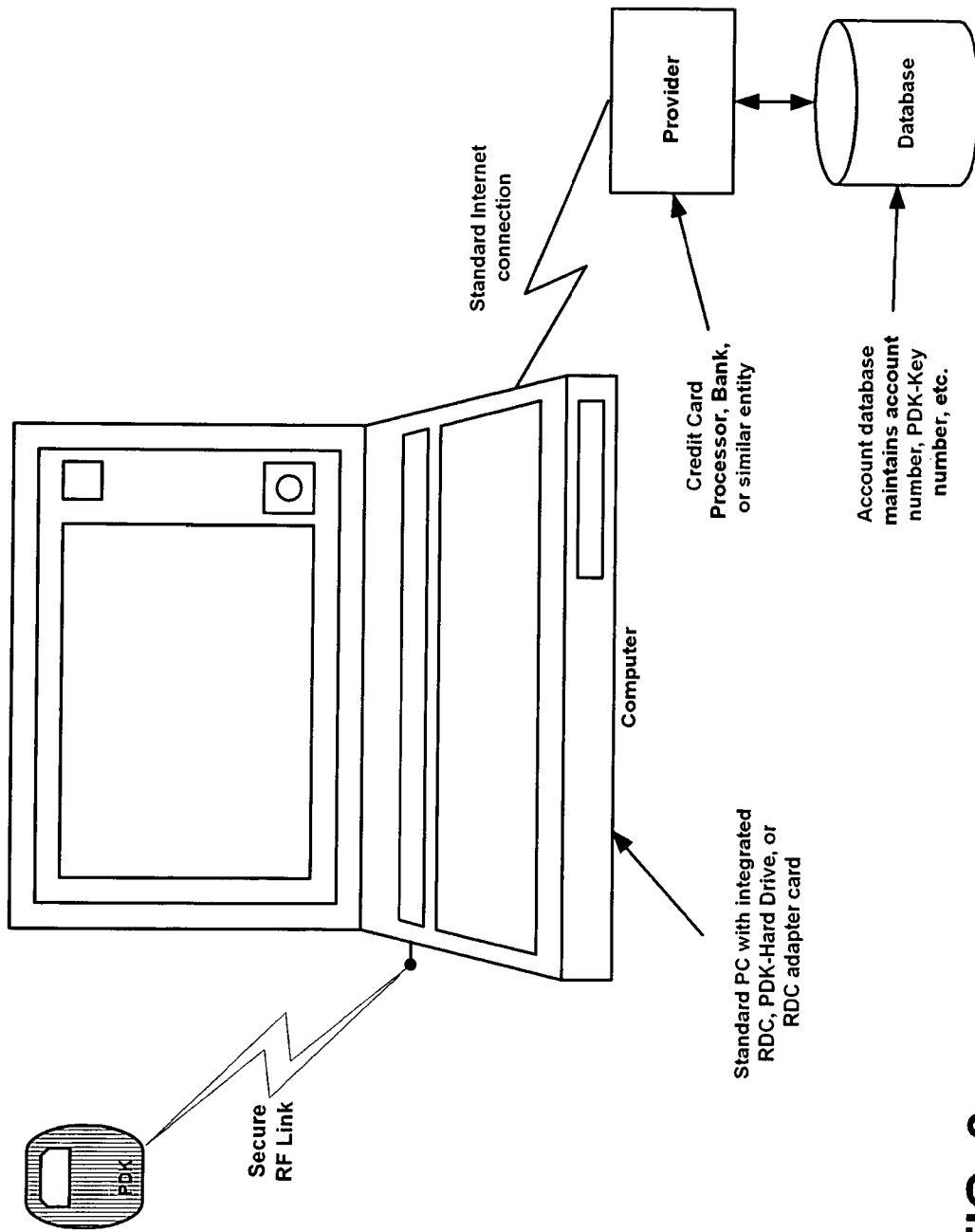


FIG. 2